IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA Plaintiff, v. "flux" a/k/a "ffhost", and "flux2" a/k/a "ffhost2", Defendants.	Civil Action No. 16-1780 **FILED *EX PARTE*** **AND UNDER SEAL**

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America has filed a complaint for injunctive relief pursuant to Title 18 U.S.C. §§ 1345 and 2521, based on the Defendants' violation of Title 18 U.S.C. §§ 1343, 1344, and 2511. The Government has also moved *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedures and Title 18 U.S.C. §§ 1345(a)(1) and 2521.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declaration, exhibits, and memorandum filed in support of the Government's Motion for a Temporary Restraining Order, Order to Show Cause and Other Ancillary Relief, the Memorandum of Law in support thereof ("Memorandum of Law"), as well as the accompanying declaration, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto. The Complaint states a

claim upon which relief may be granted against the Defendants under Title 18 U.S.C. §§ 1345 and 2511.

2. There is good cause to believe that the Defendants have engaged in and are likely to engage in acts or practices that violate Title 18 U.S.C. §§ 1343, 1344, and 2511, and that the Government is, therefore, likely to prevail on the merits of this action.

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, and 2511. The evidence set forth in the Government's Memorandum of Law and the accompanying Declaration of Special Agent Francis, demonstrate that the Government is likely to prevail on its claim that the Defendants have engaged in violations of Title 18 U.S.C. §§ 1343, 1344, and 2511 by:

a. providing a digital infrastructure for the coordination of, and communication with, hundreds of thousands of computers in the United States and elsewhere that have been intentionally infected with malicious software ("malware") to, among other things, steal banking and other online credentials from those infected computers;

b. using various malware to intercept victims' communications without authorization; and

c. using credentials stolen by the malware to access victim bank accounts and fraudulently transfer funds.

4. There is good cause to believe that if such conduct continues, it will cause irreparable harm to both individuals and businesses in the United States. There is also good

cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration and exhibits, the Government is likely to be able to prove that the Defendants are engaged in activities that violate United States law and harm members of the public, and that the Defendants have continued their unlawful conduct despite the clear injury to members of the public.

6. There is good cause to believe that providing the Defendants with advance notice of this action would cause immediate and irreparable damage to this Court's ability to grant effective final relief. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration, there is good cause to believe that – if the Defendants were to be notified in advance of this action – the Defendants would relocate their servers and/or command and control infrastructure, or otherwise implement measures to blunt or defeat the Government's planned disruption effort if informed in advance of the Government's actions.

7. The Government's request for this *ex parte* relief is not the result of any lack of diligence on the Government's part, but instead is based upon the nature of the Defendants' illegal conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), good cause and the interests of justice require that this Order be granted without prior notice to the Defendants, and accordingly, the Government is relieved of the duty to provide the Defendants with prior notice of the Government's Application.

8. The Government has demonstrated good cause to believe that Defendants have directed their illegal activity at individuals and businesses located in the Western District of Pennsylvania by, among other things, infecting numerous computers in this District with the

Nymaim/Goznym and Corebot malware campaigns and by using credentials stolen by the Nymaim/Goznym and Corebot malware campaigns to gain unauthorized access to the bank accounts of victims in this District.

9. The Government has demonstrated good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from providing this Avalanche infrastructure for the Nymaim/Goznym and Corebot malware campaigns, and other malware campaigns, to prevent further communications with existing computers infected with the various malware campaigns using the Defendant's infrastructure.

10. The Government has demonstrated good cause to believe that the Defendants have used, and will use in the future, the domain names identified in Appendices A, B, C, and D to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the various malware campaigns hosted on the Avalanche infrastructure including those involving the Nymaim/Goznym and Corebot malware. There is good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current domain names set forth in Appendix A must be immediately: 1) made inaccessible to the Defendants; and 2) the domain names redirected to the following name-servers: sc-a.sinkhole.shadowserver.org [217.160.6.63]; sc-b.sinkhole.shadowserver.org [87.106.250.34]; sc-c.sinkhole.shadowserver.org [87.106.34.1]; and, sc-d.sinkhole.shadowserver.org [87.106.86.28].

11. There is good cause to believe that the Defendants will use in the future the domain names identified in Appendix B to commit violations of 18 U.S.C. § 1343 in connection with the various malware campaigns including those using the Nymaim/Goznym and Corebot malware. There is also good cause to believe that to immediately halt the Defendants' illegal

activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' prospective domain names set forth in Appendix B must be immediately made inaccessible to the Defendants.

12. There is good cause to believe that the Defendants will use in the future the domain names identified in Appendix C to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the various malware campaigns hosted on the Avalanche architecture including those involving the Nymaim/Goznym and Corebot malware. There is also good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' prospective domain names set forth in Appendix C must be immediately made inaccessible to the Defendants by registering the domain names and redirecting the domain names to the following name servers: sc-a.sinkhole.shadowserver.org [217.160.6.63]; sc-b.sinkhole.shadowserver.org [87.106.250.34]; sc-c.sinkhole.shadowserver.org [87.106.34.1]; and, sc-d.sinkhole.shadowserver.org [87.106.86.28].

13. There is good cause to believe that the Defendants are using, and will continue to use the domain names in Appendix D to communicate with their accomplices to manage the Avalanche infrastructure. There is also good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' domain names set forth in Appendix D must be immediately made inaccessible to the Defendants by redirecting the domain names to the following name servers: donna.ns.cloudflare.com; and, paul.ns.cloudflare.com.

14. There is good cause to permit service of documents filed in this case that have been unsealed by this Court, and any unsealed Orders entered by the Court in response thereto,

as provided below, given the exigency of the circumstances, and the need for prompt relief. The following means of service, which provide due process, satisfy Fed. R. Civ. P. 4(f)(3), and are reasonably calculated to provide notice to Defendants:

a. Via email to the jabber and email addresses determined to be used by the Defendants as identified in the Declaration of Special Agent Francis; and,

b. Via publication on the Internet web site of the Department of Justice.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that the Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Andromeda, Corebot, GetTiny, Gozi2, KINS, Matsnu, Nymaim/Goznym, Ranbyus, Rovnix, TeslaCrypt, Tiny Banker aka Tinba, Trusteer App, UrlZone, VM Zeus, Vawtrak, and Xswkit, on any computers not owned by the Defendants.

IT IS FURTHER ORDERED that the Government shall participate in establishing substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law that, in conjunction with the relief ordered below, will replace the Defendants' command and control infrastructure for the identified malware families and the related botnets and sever the Defendants' connection to the infected computers in those botnets. Pursuant to the Pen Register Trap and Trace Order signed by this Court, the Government is authorized to collect dialing, routing, addressing and signaling ("DRAS") information from the

infected computers that connect to the infrastructure described in the Memorandum of Law. The Government shall ensure that no electronic content or other non-DRAS information is collected by United States law enforcement or their agents when victim computers connect to the infrastructure described in the Memorandum of Law.

IT IS FURTHER ORDERED that, with respect to any currently registered domain names set forth in Appendix A, the Domain Registries identified in Appendix E shall take the following actions with respect to the domain names for which they are the registry operator:

1. Take all reasonable measures to redirect the domain names to the substitute servers, by redirecting the domain names by changing the authoritative name servers to the following name servers: sc-a.sinkhole.shadowserver.org [217.160.6.63]; sc-b.sinkhole.shadowserver.org [87.106.250.34]; sc-c.sinkhole.shadowserver.org [87.106.34.1]; and, sc-d.sinkhole.shadowserver.org [87.106.86.28]. You are authorized, after the domain names are redirected to the substitute servers and at your discretion, to transfer the domain names in Appendix A to the Registrar of Last Resort, specifically Registrar 2482 ("RoLR"). These actions should commence no earlier than 11/30/2016 at 13:00 GMT and should conclude as soon as possible thereafter;

2. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable;

3. Prevent any further modification to, or transfer of, the domain names without the previous authorization of this Court;

4. Refrain from providing any notice or warning to, or communicating in any way with the Defendants or the Defendants' representatives and refrain from disclosing this Order

until such time as this Order is no longer under seal, except as necessary to execute this Order; and,

5. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any currently unregistered domain names set forth in Appendix B, the Domain Registries identified in Appendix E shall take the following actions with respect to the domain names for which they are the registry operator:

1. Take reasonable measures to cause the domain names in Appendix B to be unresolvable ("Blocking"). You are authorized, after the domain names are blocked, and at your discretion, to transfer existing domains to the Registrar of Last Resort, specifically Registrar 2482 ("RoLR"). These actions should commence no earlier than 11/30/2016 at 13:00 GMT and should conclude as soon as possible thereafter;

2. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable to facilitate the Blocking of these domain names;

3. Refrain from providing any notice or warning to, or communicating in any way with the Defendants or the Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order;

4. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any currently unregistered domain names set forth in Appendix C, the Domain Registries identified in Appendix E shall take the following actions with respect to the domain names for which they are registry operator:

1. Register the unregistered domain names identified in Appendix C; and,

take reasonable measures to direct the domain names to the substitute servers by assigning the newly registered domain names to the following name servers: sc-a.sinkhole.shadowserver.org [217.160.6.63]; sc-b.sinkhole.shadowserver.org [87.106.250.34]; sc-c.sinkhole.shadowserver.org [87.106.34.1]; and, sc-d.sinkhole.shadowserver.org [87.106.86.28]. You are authorized, after the domain names are redirected to the substitute servers and at your discretion, to transfer the domain names in Appendix C to the Registrar of Last Resort, specifically Registrar 2482 ("RoLR"). These actions should commence no earlier than 11/30/2016 at 13:00 GMT and should conclude as soon as possible thereafter;

2. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable;

3. Prevent any further modification to, or transfer of, the domain names without the previous authorization of this Court;

4. Refrain from providing any notice or warning to, or communicating in any way with the Defendants or the Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order.

5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to the currently registered domain names set forth in Appendix D, the Domain Registries identified in Appendix E shall take the following actions with respect to the domain names for which they are registry operator:

1. Transfer the registered domain names identified in Appendix D; and, take reasonable measures to direct the domain names to substitute servers by assigning the registered domain names to the following name servers: donna.ns.cloudflare.com; and,

paul.ns.cloudflare.com. These actions should commence no earlier than 11/30/2016 at 13:00 GMT and should conclude as soon as possible thereafter;

2. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable;

3. Prevent any further modification to, or transfer of, the domain names without the previous authorization of this Court;

4. Refrain from providing any notice or warning to, or communicating in any way with the Defendants or the Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order.

5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that copies of the Court Filings shall be served as follows:

a. Via email to the jabber and email addresses determined to be used by the Defendants as identified in the Declaration of Special Agent Francis; and,

b. Via publication on the Internet web site of the Department of Justice.

IT IS FURTHER ORDERED that pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on Dec 9, 2016 at 8:30 AM to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on the Government any answering affidavits, pleadings, motions, expert reports or declarations

and/or legal memoranda no later than two (2) days prior to the hearing on the Government's request for a preliminary injunction. The Government may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Time) on the appropriate dates listed in this paragraph.

IT IS FURTHER ORDERED that this Order shall expire on the 12th day of December 2016, at 4:00 a.m./p.m. [not to exceed 14 days], subject to the further Order of this Court.

Entered this 29th day of November, 2016 at 12:05 a.m./p.m.

Arthur J. Schwab

HON. ARTHUR J. SCHWAB
UNITED STATES DISTRICT JUDGE